VŠB - Technická univerzita Ostrava

Fakulta elektrotechniky a informatiky

Katedra Informatiky

Absolvovanie individuálnej odbornej praxe

Individual Professional Practice in the Company

2010 Ján Zahradnik

Prehlasujem, že som túto bakalársku prácu vypracoval samostatne. Uviedol som všetky literárne pramene a publikácie, z ktorých som čerpal.

V Ostrave 7. mája 2010 ….....

Podpis

Prehlásenie zástupcu spolupracujúcej právnickej alebo fyzickej osoby

Súhlasím so zverejnením tejto bakalárskej práce podľa požiadavkov č1. 26. Odst. 9 Študijného a zkúšobného poriadku pre štúdium v bakalárskych/magisterských programoch VŠB –TU Ostrava.

V Ostrave 7. mája 2010 ….....

Podpis

Ďakujem všetkým zamestnancom firmy PEGO Slovakia za odborné vedenie pri riešení úloh. Za poskytnutie cenných rád a korektúru výsledného textu. Taktiež by som rád poďakoval vedúcemu a vlastníkovi spoločnosti Pego Slovakia s.r.o Petrovi Gorekovi, že mi dal tú možnosť práce vo firme a za poskytnutie odbornej praxe v oblasti sieťových technológii.

Abstrakt

Cieľom tejto práce je podať správu o priebehu odbornej praxe vo firme PEGO Slovakia s.r.o . V úvode je uvedený profil firmy a zaradenie na pracovnú pozíciu. V nasledujúcich kapitolách sú uvedené úlohy, na ktorých som pracoval a postup ich riešenia. V závere je popísaný prínos absolvovania odbornej praxe.

Klíčová slova

PEGO Slovakia, s.r.o, odborná prax, RouterBoard, WinBox, QoS

Abstract

My bachelor work´s aim is to provide the report about how my experience in the enterprise PEGO Slovakia s.r.o. looked like. At the beginning there are a profile of the enterprise and the assignemnt into the position to be found. In the following chapters one can read the particular tasks which I was working at and the way I was solving them. At the end the contribution of taking part in the experience is described.

Key words

PEGO Slovakia, s.r.o, individual professional practice, RouterBoard, WinBox,QoS

Zoznam použitých skratiek

RTS/CTS Request to Send / Clear to Send

CSMA/CA Carrier Sense Multiple Access with Collision Avoidance

CSMA/CD Carrier Sense Multiple Access with Collision Detection

WAN Wide Area Network

LAN Local Area network

WLAN Wireless Local Area Network

SSID Service Set Identifier

IP Internet protokol

QoS Quality of Services

SFQ Stochastic Fair Queueing

BFIFO Bytes First-in-First-out

PFIFO Packet-First-in First-out

RED Random Early Detection

PCQ Per Connection Queue

HTB Hierarchical Token Bucket

Obsah

1. Úvod

1.1.Profil firmy

PEGO Slovakia, s.r.o je firma, ktorá je internetovým poskytovateľom a spoločnosťou so servisnými službami orientovanými na prácu v počítačových sieťach, budovanie bezdrôtových sietí a optických rozvodov, ale tiež poskytuje komplexné služby v oblasti IT predaj hardware a software.

1.2.Pracovné zaradenie

Po konzultácii a zvládnutí vstupných pohovorov som bol prijatý na pozíciu Servisných a konfiguračných prác a zaradený do tímu oddelenia práce s bezdrôtovými a optickými sieťami.

2.Úlohy zadané v priebehu praxe

2.1 Zoznámenie sa s RouterBoard 433 a nástrojom pre konfiguráciu WinBox

Cieľom tejto časti bolo oboznámenie sa s nástrojom pre konfiguráciu WinBoxom a samotným RouterBoardom. Pred konfiguráciou bolo nutné preštudovať dokumentáciu o samotnom module a nástroji pre konfiguráciu.

2.2 Konfigurácia smerovacieho bodu v infraštruktúre siete.

Cieľom tejto časti bolo nastaviť vysielací bod tak, aby bol možný príjem signálu a jeho vysielanie prostredníctvom ethernetového pripojenia alebo bezdrôtového pripojenia ku koncovému užívatelovi.

2.3 Riadenie prevádzky dátových tokov

Mojou úlohou bolo obmedziť dátový prenos zo servra k užívateľovi tzn. nastaviť maximálnu priepustnú rýchlosť smerom k užívateľovi (download) a taktiež aj smerom od užívateľa (upload).

2.4 Zabezpečenie kvality služby QoS

Úlohou bolo zabezpečiť kvalitu služby vytváraním pravidiel na základe, ktorých bude komunikácia usmerňovaná z hladiska priority.

2.5 Konfigurácia klientského bodu

Cieľom tejto časti bolo nastaviť prijímací bod tak, aby bol možný príjem signálu pomocou bezdrôtového prenosu.

Požadovaný výsledný stav:

- nakonfigurovať Wireless Atheros AR 5413 pre príjem signlálu
- nakonfigurovať Wireless Atheros AR 5413 pre šírenie a smerovanie signálu

- zabezpečiť správne rýchlosti dátových tokov download a upload
- vytvoriť pravidlá pre QoS
- spojenie rozhraní do virtuálneho „ethernet bridge“ rozhrania
- pripojenie koncového zariadenia na vopred nakonfigurovaný vysielací bod

3.Postup riešenia zadaných úloh

3.1 Popis konfigurácie smerovacieho bodu

Na vytvorenie bodov pre smerovanie firma používa RouterBoard RB 433. Firma vo svojej sieti používa tieto zariadenia v hlavných módoch. Prvý mód je IP smerovač, ktorý smeruje IP packety medzi sieťovými rozhraniami. Druhý mód je ethernet prepínač, pracuje na druhej vrstve OSI modelu. V tomto prípade som použil RouterBoard v móde IP smerovač, v ktorom som konfiguroval tri bezdrôtové sieťové rozhrania. Prvé bezdrôtové rozhranie som použil ako „uplink“ rozhranie (ďalej WAN), ktoré je určené na pripojenie hraničného IP smerovača do sieťovej infraštruktúry poskytovateľa. Zostávajúce sieťové rozhrania (wlan2, ether1) som pridal do jedného „virtuálneho“ sieťového rozhrania a vytvoril tak „ethernet bridge“, aby sme mohli používať rovnakú IP podsieť. Konfigurovať jednotlivé rozhrania je možné viacerými spôsobmi. Ja som používal konzolu WinBox. V RouterBoarde som vytvoril bezdrôtové rozhrania, kde pri konfigurácii prijímacej strany som zvolil názov WAN a umožnil som priradelenie fyzickej adresy k sieťovej adrese pre spolahlivé vytváranie ethernetových rámcov pomocou protokolu ARP. V záložke Wireless som zvolil mód station a frekvenčné spektrum 5GHz pásme pričom samotné frekvenčne spektrum je v rozpätí 5,3 – 5,7GHz a presne udanú frekvenciu som volil v závislosti na umiestnení, aby nedochádzalo k rušeniu s ostatnými zariadeniami pracujúcimi v tomto pásme . Security Profile, kde som určil zabezpečenie siete som zvolil WPA, kde je vyššia miera zabezpečenia než pri šifrovaní typu WEP. Na strane vysielacej som zvolil názov rozhrania wlan (x), taktiež som umožnil ARP, ale v sekcii Wireless som mód nastavil do polohy ap bridge(v tomto móde je možné spojenie point to multipoint) na vysielanie som použil frekvenčné pásmo 2,4GHz a názov ako sa sieť zobrazuje tzv. SSID podľa lokality umiestnenia.

3.2 Riadenie prevádzky dátových tokov

Na jednotlivých IP smerovačoch som zriadoval službu QoS (Quality of service) aby som zabezpečil delenie dostupnej prenosovej kapacity a prioritu jednotlivých služieb, za účelom zamedzenia zníženia kvality služieb. Ide v podstate o zabezpečenie potrebných prenosových vlastností pre prevádzku v sieti. Napríklad prenos videa je typ prevádzky, ktorý kladie vysoké nároky na kvalitu celkového prenosu. Neznesie veľké obmedzenie v oneskorení, veľkú stratu paketov, ani kolísanie oneskorenia. Preto je potrebné pri prenose videa cez počítačovú sieť tieto vlastnosti zabezpečiť. Jedným z dôležitých pravidiel QoS, ktoré som vytváral bolo vytvorenie pravidla pre spojenie, kde som obmedzoval download a upload na tomto spojení. V druhej časti som vytváral pravidlá pre rôzne typy paketov a pre prioritu ich odosielania. Pakety, určitých protokolov dostávali prednostnú prioritu odoslania, pokiaľ som ich zaradil do skupiny s najvyššou prioritou. Jednotlivé skupiny som vytváral podľa potreby zaradenia jednotlivých paketov protokolov a tak som zefektivnil celkovú kvalitu služby. MikroTik RouterOS disponuje širokými možnosťami obmedzovania a riadenia dátových tokov. Od obmedzovania jednotlivých IP adries po uprednostňovanie protokolov, portov a skupín IP adries. Z pohľadu prenosového média nedokážeme zabezpečiť stopercentnú kvalitu služieb QoS. Musíme sa preto snažiť o čo najlepší výsledok. RouterOS sa dokáže s týmto všeobecným problémom vysporiadať veľmi dobre a jeho administrátori majú k dispozícii mocný nástroj pre riadenie dátového toku tzv. Queues. Zabezpečiť kontrolu nad dátovými tokmi prechádzajúcimi smerovačmi patrí k základnej výbave IP routerov. RoutrerOS môžeme chápať ako smerovač alebo ako bridge, v oboch prípadoch je možné riadiť dátové prenosy.

Queues umožňuje ošetriť tieto nasledujúce činnosti:

- Obmedzenie rýchlosti jednotlivých IP
- Obmedzenie rýchlosti jednotlivých protokolov, portov a na nich bežiacich služieb
- Vytváranie zdielaných liniek
- Riadenie prevádzky P2P systémov

Mikrotik poskytuje niekoľko mechanizmov obmedzovania a riadenia sieťovej prevádzky.

- PFIFO (packets first-in first-out) a BFIFO (bytes first-in first-out)
- SFQ (stochastic fair queueing)
- RED (random early detection)

- PCQ (per connection queue)
- HTB (hierarchical token bucket)

PFIFO a BFIFO posiela pakety tak ako ich dostane. Všeobecne sa príliš nehodí na obmedzovanie rýchlosti mohlo by dôjst k zahlťovaniu linky. Jeho použitie je predovšetkým v oblasti štatistík.

RED je jeden z najpoužívanejších mechanizmov. Dokáže riadiť vyťaženie linky, ktorá vďaka tomu nechodí na doraz. Vlastní mechanizmi, ktoré umožňujú preniesť viac paketov.

PCQ je protokol, ktorý značným spôsobom zjednodušuje nastavenie väčšieho počtu rovnakých nezdielaných liniek. Vo vlastnostiach PCQ je potrebné nastaviť identifikátor rozpoznania jednotlivých užívateľov. Potom sa nastaví jedna queue, ktorá zahrnie rozsah IP adries, ktoré chceme obmedziť a nemusíme nastavovať pre každú IP adresu vlastné queue.

SFQ funguje na princípe pridelovania rovnomerného prenosového pásma všetkým sessions, ktoré sú otvorené. Nevýhodou tejto techniky je, že sa prideľuje pásmo jednotlivým sessions a nie priamo IP adresám.
HTB sa používa pre riadenie prevádzky, kedy chceme riadiť jednotlivé protokoly alebo porty.

Queues sú aplikované vždy v prípade, keď paket prechádza smerovačom cez dve rôzne sieťové rozhrania. Queues nie sú aplikované pri komunikácii dvoch bezdrôtových klientov v rámci jedného AP. RouterOS túto funkciu v súčasnej dobe nepodporuje. Queues sú aplikované i v prípade, že RouterOS pracuje v režime bridge.

Queues sa členia na simple queues a queues tree. Ja som som používal obmedzenie dátových tokov queue tree a to z dôvodu, že už z názvu simple queues je zrejmé, že sa jedná o základné riadenie prevádzky teda pokiaľ by sme chceli obmedziť nejakú konkrétnu IP adresu popr. rozsah IP adries v rámci subnetu siete. Queue tree mi umožňuje vytvárať zdielané linky, uprednostňovať jednotlivé protokoly alebo služby bežiace na určitých portoch. Čiže sa jedná o použitie protokolu v takom širšom spektre z pohľadu aplikovania. Tieto dve techniky je možné použiť aj paralelne tzn. skombinovať ich pre vzájomnú prevádzku. Dôležité je ale odskúšať ich z dôvodu, že v praxi platí, že sa použije prísnejšie pravidlo, ak by sa tieto prekrývali.

Pri použití Queue tree som musel najprv označiť požadované pakety, ktoré som chcel riadiť. Takéto označovanie sa nazýva mangling, ktorý sa nastavuje v sekcii **/ip firewall mangle.**

Mikrotik RouterOS má k dispozícii širokú škálu možností označovania paketov. Mojou úlohou v tejto časti bolo vytvoriť dvojicu pravidiel jedno pre upload a jedno pre download. Najprv som vytvoril prvé firewall pravidlo v mangle tabuľke, ktoré označovalo spojenie definovaným reťazcom, ktorého hodnota bola uložená v reťazci chain. Práve v tomto pravidle som definoval aj skupinu adries, na ktoré sa bude toto pravidlo vzťahovať. Action popisuje, akciu, ktorá sa má vykonať v tomto prípade je to označenie spojenia. V druhom pravidle už dochádzalo k značeniu samotných paketov v tomto spojení a taktiež hodnota reťazca bola uložená v premennnej chain.

Pre možnosť obmedzenia prenosu dát smerom k užívateľovi a od užívateľa som definoval mechanizmus obmedzenia queue type typom 'pcq', ktorý umožňuje obmedziť rozsah IP adries a nie je nutné nastavovať pre každú IP adresu vlastné queue.
Po vytvorení queue tree s názvom Download som určil hodnotu parent čo je premenná, ktorá môže nadobúdať hodnotu nadradenej queue, nejakej inej queue, rozhranie alebo jedno z dvoch virtuálnych rozhraní global-out (zahrňuje všetky odchádzajúce rozhrania) global-in (prichdzajúce rozhranie). Ja som túto hodnotu nastavil podľa pomenovaného odchádzajúceho rozhrania bridge1. V Max-limit som definoval maximálnu prenosovú rýchlosť smerom k užívateľovi.

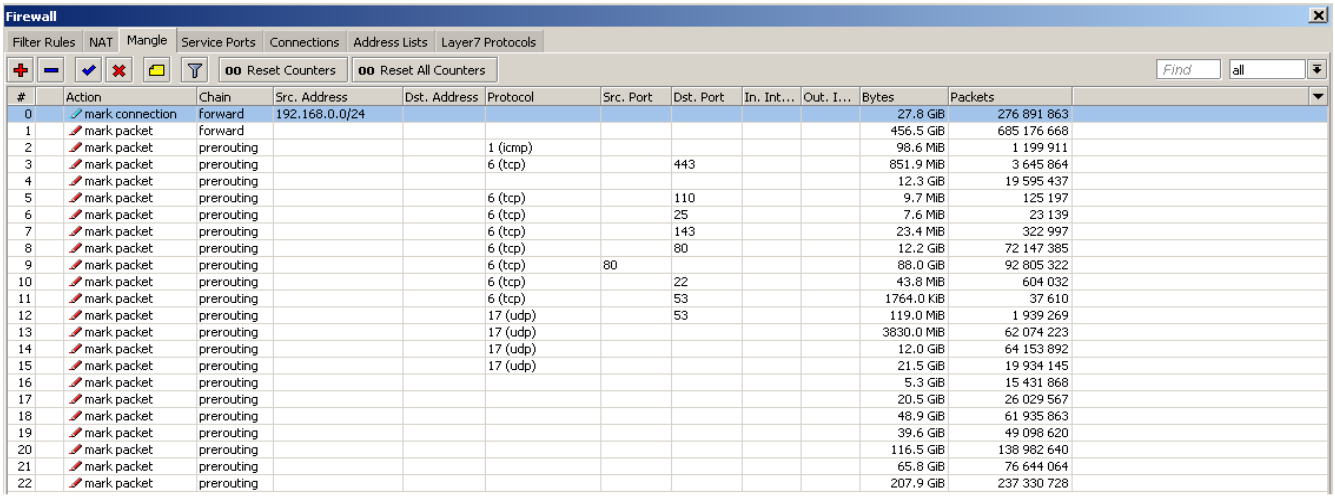
```
//označenie connections a označenie paketov v tomto connections
ip firewall mangle add chain=forward src-address=192.168.0.0/24 action=mark-connection new-connection-mark=users-con passthrough=yes
ip firewall mangle add chain=forward connection-mark=users-con action=mark-packet new-packet-mark=users passthrough=no

//definovanie mechanizmu obmedzenia
queue type add name=pcq-download kind=pcq pcq-classifier=dst-address
queue type add name=pcq-upload kind=pcq pcq-classifier=src-address

// download obmedzím uhrnne na 5.2Mb/s
queue tree add name=Download parent=bridge1 max-limit=5200000
queue tree add parent=Download queue=pcq-download packet-mark=users

// upload obmedzím uhrnne na 512kbps
queue tree add name=Upload parent=wlan1_UP_Link max-limit=512000
queue tree add parent=Upload queue=pcq-upload packet-mark=users
```

Označenie connection a označenie paketov



#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	In. Int...	Out. I...	Bytes	Packets
0	mark connection	forward	192.168.0.0/24							27.8 GiB	276 891 863
1	mark packet	forward								456.5 GiB	685 176 668
2	mark packet	prerouting			1 (icmp)					98.6 MiB	1 199 911
3	mark packet	prerouting			6 (tcp)		443			851.9 MiB	3 645 864
4	mark packet	prerouting								12.3 GiB	19 595 437
5	mark packet	prerouting			6 (tcp)		110			9.7 MiB	125 197
6	mark packet	prerouting			6 (tcp)		25			7.6 MiB	23 139
7	mark packet	prerouting			6 (tcp)		143			23.4 MiB	322 997
8	mark packet	prerouting			6 (tcp)		80			12.2 GiB	72 147 385
9	mark packet	prerouting			6 (tcp)	80				88.0 GiB	92 805 322
10	mark packet	prerouting			6 (tcp)		22			43.8 MiB	604 032
11	mark packet	prerouting			6 (tcp)		53			1764.0 KiB	37 610
12	mark packet	prerouting			17 (udp)		53			119.0 MiB	1 939 269
13	mark packet	prerouting			17 (udp)					3830.0 MiB	62 074 223
14	mark packet	prerouting			17 (udp)					12.0 GiB	64 153 892
15	mark packet	prerouting			17 (udp)					21.5 GiB	19 934 145
16	mark packet	prerouting								5.3 GiB	15 431 868
17	mark packet	prerouting								20.5 GiB	26 029 567
18	mark packet	prerouting								48.9 GiB	61 935 863
19	mark packet	prerouting								39.6 GiB	49 098 620
20	mark packet	prerouting								116.5 GiB	138 982 640
21	mark packet	prerouting								65.8 GiB	76 644 064
22	mark packet	prerouting								207.9 GiB	237 330 728

3.3 Zabezpečenie kvality služby QoS

Aby jednotlivé služby mohli dosahovať určitú kvalitu je potrebné jednotlivé pakety, ktoré prichádzajú na rozhrania IP routera označiť a zaradiť do niekoľkých skupín podľa typu paketu resp. služby, ktorá tento paket posiela tzn. určiť prioritu vybavenia požiadavku. V prvej fáze úlohy som označoval jednotlivé pakety. V sekcii /ip firewall mangle som vytvoril akciu pre značkovanie paketov reťazcom uloženým v premennej chain. Ak teda napr. paket mal hodnotu dst-port nastavenú na hodnotu 80 je zrejmé, že tento paket je posielaný protokolom http, za účelom stiahnutia webovej stránky z webového servra. Takže tento paket bol klasifikovaný názvom značky http uloženej v premennej new-packet-mark. Toto platilo aj pre ostatné porty napr. port 25 som označil značkou s názvom smtp.

// označovanie paketov pre neskorší QoS

```
ip firewall mangle add action=mark-packet chain=prerouting passthrough=no protocol=icmp new-packet-mark=icmp
ip firewall mangle add action=mark-packet chain=prerouting dst-port=443 passthrough=no protocol=tcp new-packet-mark=ssl
ip firewall mangle add action=mark-packet chain=prerouting p2p=all-p2p passthrough=no new-packet-mark=p2p
ip firewall mangle add action=mark-packet chain=prerouting dst-port=110 passthrough=no protocol=tcp new-packet-mark=pop3
ip firewall mangle add action=mark-packet chain=prerouting dst-port=25 passthrough=no protocol=tcp new-packet-mark=smtp
ip firewall mangle add action=mark-packet chain=prerouting dst-port=143 passthrough=no protocol=tcp new-packet-mark=imap
ip firewall mangle add action=mark-packet chain=prerouting dst-port=22 passthrough=no protocol=tcp new-packet-mark=ssh
```

ip firewall mangle add action=mark-packet chain=prerouting dst-port=53 passthrough=no protocol=tcp new-packet-mark=dns_tcp
ip firewall mangle add action=mark-packet chain=prerouting dst-port=53 passthrough=no protocol=udp new-packet-mark=dns_udp
ip firewall mangle add action=mark-packet chain=prerouting new-packet-mark=udp-100 packet-size=0-100 passthrough=no protocol=udp
ip firewall mangle add action=mark-packet chain=prerouting new-packet-mark=upd-500 packet-size=100-500 passthrough=no protocol=udp
ip firewall mangle add action=mark-packet chain=prerouting new-packet-mark=upd-other passthrough=no protocol=udp
ip firewall mangle add action=mark-packet chain=prerouting connection-bytes=1-512000 new-packet-mark=0bytes passthrough=yes
ip firewall mangle add action=mark-packet chain=prerouting connection-bytes=512000-1000000 new-packet-mark=1Mbyte passthrough=yes
ip firewall mangle add action=mark-packet chain=prerouting connection-bytes=1000000-3000000 new-packet-mark=3Mbyte passthrough=yes
ip firewall mangle add action=mark-packet chain=prerouting connection-bytes=3000000-6000000 new-packet-mark=6Mbyte passthrough=yes
ip firewall mangle add action=mark-packet chain=prerouting connection-bytes=60000000-0 new-packet-mark=Infinite passthrough=yes

Pre zaraďovanie paketov do priorít som potreboval najprv vytvoriť skupiny. Vytvoril som osem skupín, kde skupina číslo jedna bola skupinou s najvyššou prioritou. Pakety, ktoré sa dostali do tejto skupiny boli poslané ako prvé. Využil som typ obmedzenia queue tree, kde som označil skupinu s najvyššou prioritou s názvom PRIO1, parent som nastavil na global-in a hodnotu priority číslom 1. Tie služby, ktoré som chcel zaradiť do skupiny s prioritou 1 som v ďalšom kroku zaraďoval do stromu tak, že som vytvoril obmedzenie queue tree s menom zhodným s názvom značky a parent som nastavil hodnotou PRIO1.

Takže napr.

*queue tree add name=ICMP packet-mark=icmp parent=PRIO1 priority=*1

Obmedzenie queue tree s označením ICMP je zhodné s názvom značky paketu, ktorý splnil predpoklady, že je využívaný protokolom icmp a spadá do časti stromu s prioritou 1.

// skupina s prioritou 1

queue tree add name=PRIO1 parent=global-in priority=1
queue tree add name=ICMP packet-mark=icmp parent=PRIO1 priority=1
queue tree add name=DNS_UDP packet-mark=dns_udp parent=PRIO1 priority=1
queue tree add name=DNS_TCP packet-mark=dns_tcp parent=PRIO1 priority=1
queue tree add name=POP3 packet-mark=pop3 parent=PRIO1 priority=1
queue tree add name=SMTP packet-mark=smtp parent=PRIO1 priority=1
queue tree add name=IMAP packet-mark=imap parent=PRIO1 priority=1
queue tree add name=HTTP packet-mark=http parent=PRIO1 priority=1
queue tree add name=HTTP_down packet-mark=http_down parent=PRIO1 priority=1
queue tree add name=SSL packet-mark=ssl parent=PRIO1 priority=1
queue tree add name=SSH packet-mark=ssh parent=PRIO1 priority=1
queue tree add name=0-512 packet-mark=0bytes parent=PRIO1 priority=1

// skupina s prioritou 3

queue tree add name=PRIO3 parent=global-in priority=3

queue tree add name=1Mbyte packet-mark=1Mbyte parent=PRIO3 priority=3

// skupina s prioritou 4

queue tree add name=PRIO4 parent=global-in priority=4

queue tree add name=3Mbyte packet-mark=3Mbyte parent=PRIO4 priority=4

// skupina s prioritou 5

queue tree add name=PRIO5 parent=global-in priority=5

queue tree add name=6Mbyte packet-mark=6Mbyte parent=PRIO5 priority=5

// skupina s prioritou 6

queue tree add name=PRIO6 parent=global-in priority=6

queue tree add name=30Mbyte packet-mark=30Mbyte parent=PRIO6 priority=6

// skupina s prioritou 7

queue tree add name=PRIO7 parent=global-in priority=7

queue tree add name=60Mbyte packet-mark=60Mbytes parent=PRIO7 priority=7

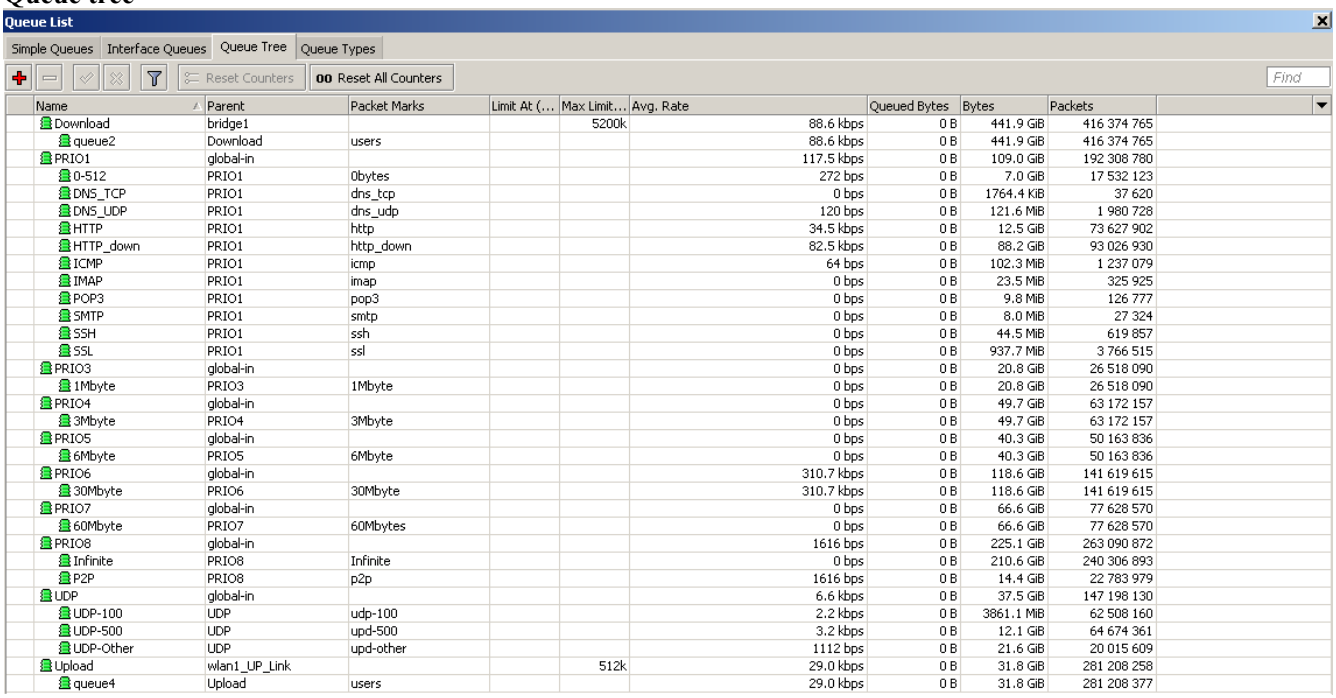
// skupina s prioritou 8

queue tree add name=PRIO8 parent=global-in priority=8

queue tree add name=P2P packet-mark=p2p parent=PRIO8 priority=8
queue tree add name=Infinite packet-mark=Infinite parent=PRIO8 priority=8

queue tree add name=UDP parent=global-in priority=1
queue tree add name=UDP-100 packet-mark=udp-100 parent=UDP priority=1
queue tree add name=UDP-500 packet-mark=upd-500 parent=UDP priority=3
queue tree add name=UDP-Other packet-mark=upd-other parent=UDP priority=8

Queue tree



Name	Parent	Packet Marks	Limit At (...	Max Limit...	Avg. Rate	Queued Bytes	Bytes	Packets
Download	bridge1			5200k	88.6 kbps	0 B	441.9 GiB	416 374 765
queue2	Download	users			88.6 kbps	0 B	441.9 GiB	416 374 765
PRIO1	global-in				117.5 kbps	0 B	109.0 GiB	192 308 780
0-512	PRIO1	0bytes			272 bps	0 B	7.0 GiB	17 532 123
DNS_TCP	PRIO1	dns_tcp			0 bps	0 B	1764.4 KiB	37 620
DNS_UDP	PRIO1	dns_udp			120 bps	0 B	121.6 MiB	1 980 728
HTTP	PRIO1	http			34.5 kbps	0 B	12.5 GiB	73 627 902
HTTP_down	PRIO1	http_down			82.5 kbps	0 B	88.2 GiB	93 026 930
ICMP	PRIO1	icmp			64 bps	0 B	102.3 MiB	1 237 079
IMAP	PRIO1	imap			0 bps	0 B	23.5 MiB	325 925
POP3	PRIO1	pop3			0 bps	0 B	9.8 MiB	126 777
SMTP	PRIO1	smtp			0 bps	0 B	8.0 MiB	27 324
SSH	PRIO1	ssh			0 bps	0 B	44.5 MiB	619 857
SSL	PRIO1	ssl			0 bps	0 B	937.7 MiB	3 766 515
PRIO3	global-in				0 bps	0 B	20.8 GiB	26 518 090
1Mbyte	PRIO3	1Mbyte			0 bps	0 B	20.8 GiB	26 518 090
PRIO4	global-in				0 bps	0 B	49.7 GiB	63 172 157
3Mbyte	PRIO4	3Mbyte			0 bps	0 B	49.7 GiB	63 172 157
PRIO5	global-in				0 bps	0 B	40.3 GiB	50 163 836
6Mbyte	PRIO5	6Mbyte			0 bps	0 B	40.3 GiB	50 163 836
PRIO6	global-in				310.7 kbps	0 B	118.6 GiB	141 619 615
30Mbyte	PRIO6	30Mbyte			310.7 kbps	0 B	118.6 GiB	141 619 615
PRIO7	global-in				0 bps	0 B	66.6 GiB	77 628 570
60Mbyte	PRIO7	60Mbytes			0 bps	0 B	66.6 GiB	77 628 570
PRIO8	global-in				1616 bps	0 B	225.1 GiB	263 090 872
Infinite	PRIO8	Infinite			0 bps	0 B	210.6 GiB	240 306 893
P2P	PRIO8	p2p			1616 bps	0 B	14.4 GiB	22 783 979
UDP	global-in				6.6 kbps	0 B	37.5 GiB	147 198 130
UDP-100	UDP	udp-100			2.2 kbps	0 B	3861.1 MiB	62 508 160
UDP-500	UDP	upd-500			3.2 kbps	0 B	12.1 GiB	64 674 361
UDP-Other	UDP	upd-other			1112 bps	0 B	21.6 GiB	20 015 609
Upload	wlan1_UP_Link			512k	29.0 kbps	0 B	31.8 GiB	281 208 258
queue4	Upload	users			29.0 kbps	0 B	31.8 GiB	281 208 377

3.4 Popis konfigurácie koncového klientského bodu

- **Základné nastavenia bezdrôtovej časti:**

Konfigurácia klientského zariadenia typu Nanostation2 L je pomerne jednoduchou záležitosťou. Prostredníctvom prístupu cez webové rozhranie bolo nutné nastaviť v bezdrôtovej časti bezdrôtový režim.Vzhľadom k tomu, že som konfiguroval koncového užívateľa tak som tento režim nastavil do polohy klient a ESSID názvom vysielacieho zariadenia, z ktorého som signál prijímal. Na zariadeniach typu NanoStation2 L je možné zvoliť módy IEEE 802.11b a IEEE 802.11g vzhľadom k tomu, že zariadenie pracuje na frekvencii 2,4GHz nie je k dispozícii mód IEEE 802.11a, ktorý je k dispozícii len na zariadeniach pracujúcich v pásme 5GHz. Pri nastavení módu na IEEE 802.11b je maximálná teoretická prenosová rýchlosť 11Mbps a šírka spektra kanálu 20MHz.

Pre nastavenie bezdrôtového zabezpečenia bolo možno použiť prístup prostredníctvom šifrovania WEP, WPA alebo WPA2. Pre bezpečný prenos informácii prostredníctvom spojenia som používal šifrovanie typu WPA2, ktoré zabezpečuje vyššiu mieru zabezpečenia než WEP a WPA.

- **WLAN sieťové nastavenie**

Pre nastavenie rozhrania WLAN v sieťovom móde router som zvolil IP adresu z rozsahu adries v podsieti vysielacieho bodu, masku, bránu pre prístup von zo siete a IP adresu primárneho doménového servra. Tieto jednotlivé nastavenia boli rôzne v závislosti od lokality pripájania koncového užívateľa.

- **Sieťové nastavenie LAN**

Pri nastavení v NanoStation2 L v sieťovom mode router som nastavil lokálnu časť siete, kde bolo potrebné zvoliť začiatok a koniec rozsahu adries, ktoré budú pridelované počítačom v lokálnej sieti a IP adresu pre prístup na toto zariadenie. Zaujímavou časťou nastavení bol Fragmentation Treshold, kde bolo potrebné určit maximálnu hodnotu prenášaného paketu v rámci siete, pri používaní viacerých prístupových techník. Vzhľadom k tomu, že štandard IEEE 802.11 je štandardom pre vnútorné siete, predpokladá sa, že väčšina klientov má vzájomnú viditeľnosť. Práve preto sa defaultne používa protokol CSMA/CA, kedy klient načúva svoju frekvenciu a vysiela, keď nikto iný nevysiela.

Lenže vo vonkajšom prostredí toto neplatí, klienti na seba nevidia takmer nikdy, takže keď sa používa defaultný protocol, tak klient predpokladá, že nikto nevysiela a začne vysielať v náhodnom čase. Čo môže viesť k tomu, že dochádza k stratám paketov a môže dôjsť aj k stratám 50% a to stačia pritom len 2 klienti. Práve z tohto dôvodu sa používa aj alternatívny protokol RTS/CTS. Pri využívaní tohto protokolu si klient vyžiada a dostane od AP určitý časový úsek, kedy môže vysielať a ostaní klienti mlčia. Tu je ale tiež jeden menší problém takáto činnosť je veľmi náročná na pásmo keby takto putovali všetky pakety znížila by sa priepustnosť siete na cca. 25%. Najefektívnejším spôsobom je využiť skutočnosť, že malé pakety je možné posielať už spomínaným CSMA/CA, kde je riziko zarušenia malé, pretože tieto pakety dokážu prejsť tak rýchlo. Hodnota RTS/CS práve udáva do akého veľkého paketu v bytoch sa má použiť CSMA/CA a od akého veľkého sa má použiť RTS/CS. Optimálna hodnota závisí na stratovosti toho, ktorého bodu. Ja som používal hodnotu 512, ktorá sa používa aj štandardne, pri viacej stratových sa používa 400 alebo menej. CSMA/CA a RTS/CTS sú dva odlišné spôsoby vysielania. Bez RTS sa ihneď pošle paket, ale pri RTS/CTS sa najprv pošle RTS požiadavok a čaká sa na CTS reply od AP. Na wireless nemôže fungovať detekcia kolízii ako na CSMA/CD, pretože to je halfduplex tzn.nie je možné vysielať a zároveň naslúchať.

4. Teoretické a praktické znalosti získané v priebehu štúdia a uplatnené v priebehu praxe.

Uplatnil jsem znalosti, které jsem dostal v predmetoch:

Počítačové siete – informácie z tohto predmetu som uplatnil pri orientovaní sa v štandardoch, ktoré sa využívajú v bezdrôtových sieťach

Práca v počítačových sieťach - znalosti z tohto predmetu mi pomohli lepšie pochopiť problematiku používania podsietí (subnetingu).

5. Znalosti a schopnosti chýbajúce v priebehu odbornej praxe

V priebehu praxe mi chýbali hlbšie skúsenosti z oblasti riadenia dátových tokov v počítačovej sieti.

6. Záver

Odobrná prax vo firme Pego Slovakia s.r.o bola pre mňa dobrou skúsenosťou. Získal som cenné skúsenosti a rady týkajúce sa bezdrôtových a počítačových sietí . Dobre som sa zoznámil s nástrojom pre konfigurovanie RouterBoard winboxom, ktorý som pri konfigurácii využíval. Naučil som sa ako sa v praxi pracuje a využíva QoS a akým spôsobom je možné riadiť prevádzku dátových tokov v počítačovej sieti pomocou RouterOS.

7. Literatura

http://wiki.mikrotik.com/wiki/Main_Page **- 2010-11-22**

http://wiki.pvfree.net/index.php/Nastaveni_RTS/CTS **- 2009-11-22**

http://download.asm.cz/inshop/prod/xtendlan/Mikrotik/EM-Mikrotik-Rizeni_datovych_toku.pdf **- 2010-03-01**

http://download.asm.cz/inshop/prod/xtendlan/Mikrotik/EM-Mikrotik-Seznameni.pdf**-2010-03-01**